UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/677,292	10/02/2000	William F. Price III	NA00-13501	4312

23419 7590 03/18/2004

COOLEY GODWARD, LLP
3000 EL CAMINO REAL
5 PALO ALTO SQUARE
PALO ALTO, CA 94306

EXAMINER
OSMAN, AHMED A

ART UNIT	PAPER NUMBER
2136	7

DATE MAILED: 03/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/677,292	**Applicant(s)** PRICE, WILLIAM F.	
	Examiner Ahmed A Osman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED OFFICE ACTION

1. Claims 1 – 27 are presented for examinations.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4, 10-13, and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,289,105 to Murota in view of US Patent No. 6,272,632 to Carman.

As per claims 1, 10, and 19:

"Identifying recipients of the email message, wherein the recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who cannot be identified by examining the email message"

Figure 5 of Murota clearly illustrates a step S18 where the receivers of the email message are identified.

"Generating a session key for the email message"

Murota teaches an encryption key generation unit 13 which is connected to a message encrypting unit 12 (Column 4 Line 28). Murota further teaches that the encryption key generation unit 13 generates an encryption key of the secret-key cryptography, which is to be used for encrypting the message (Column 4 Line 63).

"Encrypting a body of the email message with the session key"

Murota teaches a message encrypting unit 12, which encrypts the message by using this encryption key according to the secret-key cryptography (Column 5 Line 1).

"Creating a recipient block for the email message that contains an entry for each recipient of the email message"

Figure 4 of Murota clearly illustrates a block dedicated to the receivers of the message. It further illustrates a separate block for each recipient.

"Wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key, so that only a corresponding private key held by the recipient can be used to decrypt the encrypted session key."

Murota teaches an encryption unit 16, which encrypts the encryption key according to the public-key cryptography by using each receiver's public key and sender key (Column 5 Line 38).

"Wherein each entry additionally contains an identifier for the associated public key, so that each recipient can determine whether the recipient possesses the corresponding private key that can decrypt the encrypted session key"

Murota teaches a receiver information 33, which describes information obtained by encrypting the message encryption key according to the public-key cryptography by using each receiver's public key (Column 6 Line 9). Murota further teaches that the receiver can obtain the encryption key of the email by decrypting his own encryption key information by using the secret key in his own possession and decrypt the email message by using the encryption key so obtained (Column 6 Line 24). The office interprets the receiver's encryption key information as an identifier for each encryption key so that each recipient can match the information to the information he posses to decrypt the session key. Furthermore, Carman teaches an encrypting system that generates a key recovery field (KRF) (Column 2 Line 22). The KRF includes an unencrypted header section and an encrypted payload section (Column 2 Line 55). The unencrypted header section includes a key identifier (KI) (Column 2 Line 59). The key identifier uniquely identifies the public key used to encrypt the payload section (Column 2 Line 61). Moreover Carman teaches that the encrypted payload section 1020 of KRF

1000 is encrypted using KRCpub (public key). The corresponding KRCpriv (private key) is stored in key recovery center (KRC) 110 and is identified by the information contained in KRC identifier field 1011 and key identifier field 1012 of unencrypted header section 1010 (Column 12 Line 41).

"Wherein identifiers for public keys belonging to known recipients are statistically unique."

Carman teaches that the KRC identifier field 1011 and the key identifier field 1012 can include various types of information that would uniquely identify the KRC and the KRCpub that is used to encrypt payload section 1020 (Column 12 Line 41).

"Wherein identifiers for public keys belonging to anonymous recipients are not statistically unique."

Carman teaches an access rule index (ARI) that is included in the unencrypted header section (Column 17 Line 51). ARI can appear as cleartext because the ARI does not represent authentication information. Knowledge of the ARI by a potential decryptor will not enhance the decryptor's chances of gaining unauthorized access to the user secret encrypted within the KRF because the ARI merely represents an index to an access rule. The ARI does not itself represent authentication information. In other words, this alternative KRF format is permissible because the ARI does not represent actual authentication information that will be directly used by the KRC 110 in determining whether a potential decryptor is authorized to receive the user secret

(Column 17 Line 54). Carman further teaches an example (Column 18 Lines 12-17) where based on inspection of at least the cleartext ARI, a potential decryptor selects the KRF.sub.i that the potential decryptor knows is associated with him. More specifically, the potential decryptor selects the KRF.sub.i that includes the ARI.sub.i that the potential decryptor knows references an AR that the potential decryptor can satisfy. This selected KRF.sub.i is then sent to the appropriate KRC (Column 18 Line 27).

"Sending the email message to the recipients"

Murota teaches a method and apparatus that comprises a sender S and receivers A and B where the email indicates that it is destined from Sender S to receivers A and B (Column 4 Line 45).

Murota does not specifically disclose that the identifiers for public keys are statistically unique or not. It would have been obvious to one ordinarily skilled in the art at the time the invention was made to modify Murota's invention to include identifiers that are statistically unique for know recipients and not statistically unique for anonymous recipients. One would have been motivated to make such a modification in light of LeBourgeois's teachings that public keys thereby gradually accumulate sufficient "mass" to vouch for the identity of the owner of the public key (Column 2 Line 46). Therefore the modification permits flexible authorization-type certification while preserving the privacy of individual users (Column 3 Line 40).

As per claims 2, 11, and 20:

> **"Wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to decrypt the body of the email message."**

Carman teaches an access rule index (ARI) that is included in the unencrypted header section (Column 17 Line 51). ARI can appear as cleartext because the ARI does not represent authentication information. Knowledge of the ARI by a potential decryptor will not enhance the decryptor's chances of gaining unauthorized access to the user secret encrypted within the KRF because the ARI merely represents an index to an access rule. The ARI does not itself represent authentication information. In other words, this alternative KRF format is permissible because the ARI does not represent actual authentication information that will be directly used by the KRC 110 in determining whether a potential decryptor is authorized to receive the user secret (Column 17 Line 54). Carman further teaches an example (Column 18 Lines 12-17) where based on inspection of at least the cleartext ARI, a potential decryptor selects the KRF.sub.i that the potential decryptor knows is associated with him. More specifically, the potential decryptor selects the KRF.sub.i that includes the ARI.sub.i that the potential decryptor knows references an AR that the potential decryptor can satisfy. This selected KRF.sub.i is then sent to the appropriate KRC (Column 18 Line 27).

As per claims 3, 12, and 21:

"Wherein an identifier for a public key is formed by creating a hash of the public key."

Murota does not specifically state that the identifier is the hash of the public key. Fischer teaches an invention which incorporates into a certificate a hash of an original signer's public key or certificate, as well as an indication (generally either the hash of the public key or certificate, but possibly some other abstract identifier or group code) of the other entities who are allowed to also sign the certificate (Column 13 Line 56). It would have been obvious to one ordinarily skilled in the art at the time the invention was made to modify Murota's invention to include identifiers that are the hashes of the public key. One would have been motivated to make such a modification in light of Fischer's teachings that including an identifier that is the hash of the public key operates to prevent "just anyone" from adding their signature to an existing certificate (in which case they might then appear to be authorized to cancel it) (Column 13 Line 52).

As per claims 4, 13, and 22:

"Wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique."

"Whereby the identifier cannot be used to uniquely identify the anonymous recipients."

"Whereby a recipient can use the identifier to exclude a large percentage of all possible corresponding public keys held by the recipient form matching the identifier."

Carman teaches an access rule index (ARI) that is included in the unencrypted header section (Column 17 Line 51). ARI can appear as cleartext because the ARI does not represent authentication information. Knowledge of the ARI by a potential decryptor will not enhance the decryptor's chances of gaining unauthorized access to the user secret encrypted within the KRF because the ARI merely represents an index to an access rule. The ARI does not itself represent authentication information. In other words, this alternative KRF format is permissible because the ARI does not represent actual authentication information that will be directly used by the KRC 110 in determining whether a potential decryptor is authorized to receive the user secret (Column 17 Line 54). Carman further teaches an example (Column 18 Lines 12-17) where based on inspection of at least the cleartext ARI, a potential decryptor selects the KRF.sub.i that the potential decryptor knows is associated with him. More specifically, the potential decryptor selects the KRF.sub.i that includes the ARI.sub.i that the potential decryptor knows references an AR that the potential decryptor can satisfy. This selected KRF.sub.i is then sent to the appropriate KRC (Column 18 Line 27).

4. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,289,105 to Murota as applied to claims 1, 10, and 19 above, and in view of US Patent No. 6,170,744 to Lee.

As per claims 5, 14, and 23:

> **"Encrypting the body of the email message, including a checksum into the body of the email message, so that a recipient can examine the checksum to verify that the correct private key was used in decrypting the email message."**

Murota does not specifically disclose that a checksum is included in the method that involves a checksum. Lee teaches a method that includes a step of computing a check sum on the decrypted data symbol. The method further includes a step of comparing the computed check sum with a check sum value included in the data symbol and retrieved from the data symbol through the decrypting of the data symbol to determine if the decrypted data symbol is error free. The method still further includes a step of verifying a digital signature provided with the data symbol using a public digital signature key. If the comparison in the third step and the verification in the fourth step are successful, the data symbol is authenticated and validated (Column 21). Therefore it would have been obvious to one ordinarily skilled in the art to modify Murota's invention to include a checksum to authenticate the message in light of Lee's suggestion that one-way hashes are utilized in data communications systems to prevent what can be thought of as the "digital cloning" of data. One-way hashing is a process whereby a hash value is mathematically processed to recreate the original data. One-way hashes mathematically ensure that the transformation that produced the unique hash value cannot be used in a reverse process. Furthermore, one-way hashing equations have been developed for which it is computationally impossible to determine two values that produce the same hash value. These types of one-way hashing equations are used in inventions to provide a fool-proof fraud prevention and authentication system and method (Column 7).

5. Claims 6-9, 15-18, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,289,105 to Murota in view of US Patent No. 6,272,632 to Carman, and further in view of US Patent No. 6,170,744 to Lee.

As per claims 6, 15, and 24:

"Receiving the email message at a recipient, where in the email message includes:

A message body that has been encrypted with a session key"

Murota teaches an encryption key generation unit 13 which is connected to a message encrypting unit 12 (Column 4 Line 28). Murota further teaches that the encryption key generation unit 13 generates an encryption key of the secret-key cryptography, which is to be used for encrypting the message (Column 4 Line 63). Murota teaches that the message-encrypting unit 12 encrypts the message by using this encryption key according to the secret-key cryptography (Column 5 Line 1).

"A recipient block that contains an entry for each recipient of the email message"

Figure 4 of Murota clearly illustrates a block dedicated to the receivers of the message. It further illustrates a separate block for each recipient.

"Wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key"

Murota teaches an encryption unit 16, which encrypts the encryption key according to the public-key cryptography by using each receiver's public key and sender key (Column 5 Line 38).

"Wherein each entry additionally contains an identifier for the associated public key"

Carman teaches an encrypting system that generates a key recovery field (KRF) (Column 2 Line 22). The KRF includes an unencrypted header section and an encrypted payload section (Column 2 Line 55). The unencrypted header section includes a key identifier (KI) (Column 2 Line 59). The key identifier uniquely identifies the public key used to encrypt the payload section (Column 2

Line 61). Moreover Carman teaches that the encrypted payload section 1020 of KRF 1000 is encrypted using KRCpub (public key). The corresponding KRCpriv (private key) is stored in key recovery center (KRC) 110 and is identified by the information contained in KRC identifier field 1011 and key identifier field 1012 of unencrypted header section 1010 (Column 12 Line 41).

"Wherein identifiers for public keys belonging to known recipients are statistically unique."

Carman teaches that the KRC identifier field 1011 and the key identifier field 1012 can include various types of information that would uniquely identify the KRC and the KRCpub that is used to encrypt payload section 1020 (Column 12 Line 41).

"Wherein identifiers for public keys belonging to anonymous recipients are not statistically unique."

Carman teaches an access rule index (ARI) that is included in the unencrypted header section (Column 17 Line 51). ARI can appear as cleartext because the ARI does not represent authentication information. Knowledge of the ARI by a potential decryptor will not enhance the decryptor's chances of gaining unauthorized access to the user secret encrypted within the KRF because the ARI merely represents an index to an access rule. The ARI does not itself represent authentication information. In other words, this alternative KRF format is permissible because the ARI does not represent actual authentication information that will be directly used by the KRC 110 in determining whether a potential decryptor is authorized to receive the user secret (Column 17 Line 54). Carman further teaches an example (Column 18 Lines 12-17) where based on inspection of at least the cleartext ARI, a potential decryptor selects the KRF.sub.i that the potential decryptor knows is associated with him. More specifically, the potential decryptor selects the KRF.sub.i that includes the ARI.sub.i that the potential decryptor knows references an AR that the potential decryptor can satisfy. This selected KRF.sub.i is then sent to the appropriate KRC (Column 18 Line 27).

Murota does not specifically disclose that the identifiers for public keys are statistically unique or not. It would have been obvious to one ordinarily skilled in the art at the time the invention was made to modify Murota's invention to include identifiers that are statistically unique for know recipients and not statistically unique for anonymous recipients. One would have been motivated to make such a modification in light of LeBourgeois's teachings that public keys thereby gradually accumulate sufficient "mass" to vouch for the identity of the owner of the public key (Column 2 Line 46). Therefore the modification permits flexible authorization-type certification while preserving the privacy of individual users (Column 3 Line 40).

"Attempting to match a candidate public key held by the recipient with key identifier in the recipient block, if the candidate public key matches a key identifier, decrypting the associated encrypted session key using an associated private key to restore the session key"

Murota teaches that the receiver of the electronic email can obtain the encryption key of the electronic mail message by decrypting his own encryption key information by using his own secret key in his own possession (Column 6 Line 24).

"Decrypting the message body using the session key"

Murota teaches that the receiver of the electronic email can obtain the encryption key of the electronic mail message by decrypting his own encryption key information by using his own secret key in his own possession. Murota further teaches that the receiver can then decrypt the electronic email message by using the encryption key so obtained (Column 6 Line 24).

"Examining a checksum in the message body to verify that message body was correctly decrypted"

Murota does not specifically disclose that a checksum is included in the method that involves a checksum. Lee teaches a method that includes a step of computing a check sum on the decrypted data symbol. The method further includes a step of comparing the computed check sum with a check sum value included in the data symbol and retrieved from the data symbol through the decrypting of the data symbol to determine if the decrypted data symbol is error free. The method still further includes a step of verifying a digital signature provided with the data symbol using a public digital signature key. If the comparison in the third step and the verification in the fourth step are successful, the data symbol is authenticated and validated (Column 21). Therefore it would have been obvious to one ordinarily skilled in the art to modify Murota's invention to include a checksum to authenticate the message in light of Lee's suggestion that one-way hashes are utilized in data communications systems to prevent what can be thought of as the "digital cloning" of data. One-way hashing is a process whereby a hash value is mathematically processed to recreate the original data. One-way hashes mathematically ensure that the transformation that produced the unique hash value cannot be used in a reverse process. Furthermore, one-way hashing equations have been developed for which it is computationally impossible to determine two values that produce the same hash value. These types of one-way hashing equations are used in inventions to provide a fool-proof fraud prevention and authentication system and method (Column 7).

As per claims 7, 16, and 25:

> **Identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to decrypt the body of the email message."**

Carman teaches an access rule index (ARI) that is included in the unencrypted header section (Column 17 Line 51). ARI can appear as cleartext because the ARI does not represent authentication information. Knowledge of the ARI by a potential decryptor will not enhance the decryptor's chances of gaining unauthorized access to the user secret encrypted within the KRF because the ARI merely represents an index to an access rule. The ARI does not itself represent authentication information. In other words, this alternative KRF format is permissible because the ARI does not represent actual authentication information that will be directly used by the KRC 110 in determining whether a potential decryptor is authorized to receive the user secret (Column 17 Line 54). Carman further teaches an example (Column 18 Lines 12-17) where based on inspection of at least the cleartext ARI, a potential decryptor selects the KRF.sub.i that the potential decryptor knows is associated with him. More specifically, the potential decryptor selects the KRF.sub.i that includes the ARI.sub.i that the potential decryptor knows references an AR that the potential decryptor can satisfy. This selected KRF.sub.i is then sent to the appropriate KRC (Column 18 Line 27).

As per claims 8,17, and 26:

"Wherein an identifier for a public key is formed by creating a hash of the public key."

Murota does not specifically state that the identifier is the hash of the public key. Fischer teaches an invention which incorporates into a certificate a hash of an original signer's public key or certificate, as well as an indication (generally either the hash of the public key or certificate, but possibly some other abstract identifier or group code) of the other entities who are allowed to also sign the certificate (Column 13 Line 56). It would have been obvious to one ordinarily skilled in the art at the time the invention was made to modify Murota's invention to include identifiers that are the hashes of the public key. One would have been motivated to make such a modification in light of Fischer's teachings that including an identifier that is the hash of the public key operates to prevent "just anyone" from adding their signature to an existing certificate (in which case they might then appear to be authorized to cancel it) (Column 13 Line 52).

As per claims 9, 18, and 27:

> **"Wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique."**
>
> **"Whereby the identifier cannot be used to uniquely identify the anonymous recipients."**
>
> **"Whereby a recipient can use the identifier to exclude a large percentage of all possible corresponding public keys held by the recipient form matching the identifier."**

Carman teaches an access rule index (ARI) that is included in the unencrypted header section (Column 17 Line 51). ARI can appear as cleartext because the ARI does not represent authentication information. Knowledge of the ARI by a potential decryptor will not enhance the decryptor's chances of gaining unauthorized access to the user secret encrypted within the KRF because the ARI merely represents an index to an access rule. The ARI does not itself represent authentication information. In other words, this alternative KRF format is permissible because the ARI does not represent actual authentication information that will be directly used by the KRC 110 in determining whether a potential decryptor is authorized to receive the user secret (Column 17 Line 54). Carman further teaches an example (Column 18 Lines 12-17) where based on inspection of at least the cleartext ARI, a potential decryptor selects the KRF.sub.i that the potential decryptor knows is associated with him. More specifically, the potential decryptor selects the KRF.sub.i that includes the ARI.sub.i that the potential decryptor knows references an AR that the potential decryptor can satisfy. This selected KRF.sub.i is then sent to the appropriate KRC (Column 18 Line 27).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents and patent application publications are cited to further show the state of the art with respect to secure email processing systems in general:

U.S. Patent No. 5,081,678 to Kaufman et al.

U.S. Patent No. 5,214,702 to Fischer

U.S. Patent No. 5,481,613 to Ford et al.

U.S. Patent No. 5,812,670 to Micali

U.S. Patent No. 5,852,665 to Gressel et al.

U.S. Patent No. 5,958,005 to Thorne et al.

U.S. Patent No. 6,026,166 to LeBourgeois

U.S. Patent No. 6,161,129 to Rochkind

U.S. Patent No. 6,314,190 to Zimmermann

U.S. Patent No. 6,401,203 to Eigeles

U.S. Patent No. 6,442,687 to Savage

U.S. Patent No. 6,584,564 to Olkin et al.

U.S. Patent No. 6,591,291 to Gabber et al.

U.S. Patent No. 6,608,888 to Bedingfield et al.

U.S. Patent No. 6,611,812 to Hurtado et al.

U.S. Patent No. 6,628,786 to Dole

U.S. Patent No. 6,640,301 to Ng

U.S. Patent No. 6,675,153 to Cook et al.

U.S. Patent Application Publication No. 2002/0007453 to Nemovicher

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmed A Osman whose telephone number is 703-305-8910. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

***

Ahmed Osman

United States Patent & Trademark Office

Patent Examiner – AU 2136

March 3, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100